# An Annotated Table of Contents

of

# HACKERS' WARS: How the FBI, Pentagon, NATO and technologists staged the Arab Spring and resulting coups and wars

## Or, How I Learned to Worry and Stop Loving the Arab Spring: an argument in favor of cyber realism

Joanna Bell, M.A. Near Eastern Languages and Cultures, Ph.D. Coursework Completed

**Acknowledgements**

This paper is several years delayed in being written. I began the research process in 2015 as an idea for a possible Ph.D. dissertation topic while living in Washington, D.C. My research included looking at material from the hacking group Anonymous on social media, attending a conference held by the US State Department on the Georgetown University campus in July 2016 titled "Threats to Religious and Ethnic Minorities Under the Islamic State", and making contact with a former employer who served as a White House advisor on the Middle East under George W. Bush. By the end of summer 2016, after less than a year researching the topic of US involvement in the Arab Spring, I had received threats at my home and was under heavy cyber surveillance.

Unwilling to let my efforts go to waste, I have produced this paper from that research. This research was produced freely for free, under no auspices of any institution or individual, and can be shared freely for free with proper attribution to the author.

**Abstract**

Draft of a working paper arguing that the Arab Spring and its resulting coups and wars across the Middle East were orchestrated by US law enforcement, intelligence, and the military establishment with the willing and knowing cooperation of hacker groups like Anonymous, big technology companies, major media outlets, and major policy institutions.

**Hackers' wars** are information operations[1] incorporating electronic warfare operations[2] conducted by a state which deliberately involve populations to effect war, coup, or other conditions of life calculated to bring about physical destruction. These operations are typically carried out as wargames before or simultaneously with the execution of the real-world operation. The most salient features of hackers' wars are propaganda efforts, surveillance, cyberespionage and hacking, electronic weaponry deployment, and, importantly, the misattribution of these cyber coercion and deterrence techniques. The role of cyberweaponry is most saliently concealed in hackers' wars because information operations, as "U.S. policy suggests[,] these types of operations fall below the threshold of armed conflict," and are therefore not "considered an armed attack under international law" or "an act of war". As professor of strategy Sean McFate has put it, "irregular warfare manufactures the fog of war" present in wars of armed conflict; conversely, DARPA's Information Processing Techniques Office repeated adage maintains "Information lifts the fog of war". In short, **hackers' wars are the wars brought about by hackers.** The Arab Spring is addressed as hackers' wars in this present study.

[1] From Congressional Research Service *Defense Primer: Information Operations*: While there is currently no official U.S. government (USG) definition of information warfare (IW), practitioners typically conceptualize it as a strategy for the use and management of information to pursue a competitive advantage, including both offensive and defensive operations… which include computer network attack, computer network defense, and computer network exploitation; psychological operations (PSYOP); electronic warfare (EW); operations security (OPSEC); and military deception (MILDEC).

[2] From Congressional Research Service *Defense Primer: Electronic Warfare*: Electronic warfare (EW), as defined by the Department of Defense (DOD), are military activities that use electromagnetic energy to control the electromagnetic spectrum ("the spectrum") and attack an enemy… Applications include radio frequencies to communicate with friendly forces; microwaves for tactical data-links, radars, and satellite communications; infrared for intelligence and to target enemies; and lasers across the entire spectrum to communicate, transmit data, and potentially destroy a target.

This study looks at current events, social media, scholarly publications, cyber technology, and media trends, adapting an approach of cyber realism to the Arab Spring conversation within Max Weber's political theory of monopolies on violence and legitimate infringements. This approach emphasizes technical aspects and larger trends in cyber-politics, current events as products of the US wargame and intelligence industries. Clausewitz's social structure of war triad is applied by identifying those with end-to-end control of the popular passions, operational instruments, and policy decisions of war. All of these aspects are considered in order to give a timely answer to the current international security crises of media revolutions and cyberterrorism.

**Timeline**

May 2001

Wargame *UV '01* simulates US war in landlocked Central Asia prompted by Islamic terror attack

Sept. 11, 2001

Wargames scheduled morning of 9/11 simulate plane hijackings, NORAD unable to respond in scenario

Sept. - Oct. 2001

Gen. Clark learns Rumsfeld's orders to 'take out' Iraq, Syria, Lebanon, Somalia, Sudan, Iran; US invades Afghanistan

July - Aug. 2002

Wargame *MC '02* simulates removal of Middle East regime with weapons of mass destruction

Mar. 2003

US invades Iraq on premise it has weapons of mass destruction

Jan. 2007

US begins bombing Al-Shabab in Somalia

2008 - 2011

Facebook, Google, MTV & US NGOs begin training Arab protesters in social media protest methods

Nov. 2008

National Intel. Council report predicts emergence of coronavirus pandemic by 2025 will kill hundreds of millions worldwide

2009

Iran election protests coordinate via social media; Electronic Frontier Foundation crowd sources US hacking of Iranian social media accounts

Hackers use Iranian proxies to join Iranian social media protests

Late 2000s

Ret. Army officer witnesses RAND Corp. plans to flood Arab social media with 'democracy' & 'revolution' tags

Mid- 2010

Google Exec. Wael Ghonim creates "We Are All Khalid Said" Facebook page & gains large Egyptian following

Dec. 2010

Anonymous given IRC #InternetFeds, chat focuses on revolution in Middle East

FBI uses Anonymous asset to start chat on Occupy Wall Street movement

Dec. 9, 2010

Anonymous IRCs & bot armies disappear after plans to hack Amazon.com

Jan. 2011

Anonymous reconnects Arab Spring protesters' Internet after gov'ts shut it down, stages Occupy Wall Street protests

Arab Spring protests break out coordinated via social media; Google Exec. Ghonim publicly attends Egyptian protests

Jan. 14, 2011

Tunisian revolution coordinated via social media leads to President Ben Ali's resignation

Feb. 2011

Egyptian revolution coordinated via social media leads to President Mubarak's resignation; Revolution via social media breaks out in Libya

Mar. 2011

NATO invades Libya; US backs rebels as Syrian War begins

July 8-9, 2011

UN peacekeepers enter southern Sudan one day before the Sudan partitions into South Sudan and Sudan

Oct., Dec. 2011

UN & NATO-backed Libyan forces capture and kill Gaddafi; US withdraws from Iraq

2012 - 2013

Former CIA officer and NSA contractor Snowden gives classified files to journalist Glen Greenwald

Mar. 2013

Saudi prince Salman bin Sultan & NSA direct Syrian rebels to 'flatten' Damascus

July 4, 2014

US 1st bombs ISIS camp in Syria attempting to find hostaged US journalists & NGO worker

Mid- 2014

ISIS gains large social media recruiting presence in the West via social media and declares "Caliphate"

Oct. 24, 2017

Glen Greenwald & media outlet *The Intercept* reveal four year-old 'Snowden file' that warned of Saudi & US-led destruction of Damascus

Dec. 2018 – Apr. 11, 2019

Revolution in Sudan coordinated via social media leads to President al-Bashir's resignation, Bashir goes on trial at ICC for crimes against humanity

Oct. 2019

The Gates Foundation, Johns Hopkins University, and The World Economic Forum stage *Event 201*, a tabletop exercise simulating severe pandemic

Oct. 17 - 29, 2019

Revolution in Lebanon coordinated via social media leads to Prime Minister Hariri's resignation

Mar. 2020

The World Health Organization declares Coronavirus-19 a global pandemic

Aug. 2020

Prime Minister Hassan Diab and entire Lebanese gov't resign following Beirut explosion & protests

Jan. 2021

US election protests coordinated via social media lead to storming of US Capitol building and 2nd impeachment of
President Donald Trump

July 2021

Coronavirus-19 death toll reaches 4.09 million worldwide

**Abstract**

Draft of a working paper arguing that the Arab Spring and its resulting coups and wars across the Middle East were orchestrated by US law enforcement, intelligence, and the military establishment with the willing and knowing cooperation of hacker groups like Anonymous, big technology companies, major media outlets and major policy institutions.

Hackers' wars are irregular warfare information operations incorporating electronic warfare operations conducted by a state which deliberately involve populations to effect war, coup, or other conditions of life calculated to bring about physical destruction. These operations are typically carried out as wargames before or simultaneously with the execution of the real-world operation. The most salient features of hackers' wars are propaganda efforts, surveillance, cyberespionage and hacking, electronic weaponry deployment, and, importantly, the misattribution of these cyber coercion and deterrence techniques. The role of cyberweaponry is most saliently concealed in hackers' wars because information operations, as "U.S. policy suggests[,] these types of operations fall below the threshold of armed conflict," and are therefore not "considered an armed attack under international law" or "an act of war". As professor of strategy Sean McFate has put it, "irregular warfare manufactures the fog of war" present in wars of armed conflict; conversely, DARPA's Information Processing Techniques Office repeated adage maintains "Information lifts the fog of war". In short, hackers' wars are the wars brought about by hackers. The Arab Spring is addressed as hackers' wars in this present study.

This study looks at current events, social media, scholarly publications, cyber technology, and media trends, adapting an approach of cyber realism to the Arab Spring conversation. Applying Max Weber's political theory of monopolies on violence and legitimate infringements to cyber politics, this approach emphasizes technical aspects and current events as products of the US wargame and intelligence industries. Clausewitz's social structure of war triad is applied to the cyber domain, identifying those with end-to-end control of the popular passions, operational instruments, and policy decisions of war. All of these aspects are considered in order to give a timely answer to the current international security crises of media revolutions and cyberterrorism.

**Introduction**

I analyze the processes that created revolution, war, and genocide in the age of the cyberarms race and Web 2.0. I focus on the intersection between information technology and US foreign policy in the Middle East as an information science professional and Middle East studies expert. This is in no way a look at 'what went wrong' in the celebrated Arab Spring movement, and where my opinion is expressed, it is intolerant of the exclusion of the devastating results of the Arab Spring.

It is a laying out of facts as they occurred with, first, knowledge of the US' military and intelligence transgressions in the Middle East, and second, a basic understanding of the history of technology in modern war crimes. It shows that the events that have unfolded before and since 2011 display a high level of strategic and tactical coordination between government and industry professionals to the end seen today.

**Hackers' wars** are irregular warfare information operations incorporating electronic warfare operations conducted by a state which deliberately involve populations with the aim of effecting war, coup, or other conditions of life calculated to bring about physical destruction.. The most salient features of hackers' wars are surveillance, cyberespionage and hacking, and electronic weaponry deployment, and, importantly, the misattribution of these cyber coercion and deterrence techniques. The role of cyberweaponry is most saliently concealed in hackers' wars because information and psychological operations, as "U.S. policy suggests[,] these types of operations fall below the threshold of armed conflict," and are therefore not

"considered an armed attack under international law" or "an act of war". The Arab Spring is addressed as hackers' wars in this present study.

Theoretically, the present study is a work of realism and therefore it "assume[s] unitary governmental decision-making with a high degree of control over implementation and access to near-perfect information" over "popular passions, operational instruments, and political objectives". This created the monopolies of violence that were needed to bring about both the idealism of the Arab Spring and the devastation that would result. As Karolak writes in *The Social Media Wars*, the government is "simultaneously target, sponsor, and antagonist for social movements as well as the organizer of the political system and the arbiter of victory." Simply put, the Arab Spring was war profiteering and pre-existing policy enacted via social engineering.

**2011 in 20/20**

A decade after 2011, I highlight, with a cyber realist approach, the crimes against humanity which proceeded from the Arab Spring.

On the Mediterranean, very near Tunisia, slave auctions are now held in Tripoli, Libya. Following the NATO attack on Libya, slave markets emerged out of refugee camps where Libyan and other Africans have attempted to go north to escape yet another 'failed' state at the hands of NATO.

Similarities suggest that the ISIS sex slave trade functions within the existing sex trafficking markets as they have existed for decades in the US. Technologists, the FBI and Pentagon's involvement in human trafficking and tracking is discussed. It is also noted that the US has repeatedly taken military action to support the expansion of ISIS and therefore its institutionalized sex slavery market. It has been confirmed that ISIS trades so-called sex slaves via the Internet. The industries which profit off of what Jean Baudrillard called "televised holocausts" are the major issue discussed throughout every section of this book.

In 2014, a UN official was questioned in a press conference about medical crimes taking place in Turkish hospitals and refugee camps. Estimates of up to 18,000 Syrian children have been medically executed or allowed to die in order for their organs to be harvested and sold.

Accounts of the crimes taking place in Syrian detention facilities show that complicit media technologists and the US State Department have contradicted their own narratives by claiming lack of access to information on crimes taking place at Saydnaya military torture prison and crematoria which people are transported to by "meat fridge trucks" and where bodies are cremated and buried in mass graves. It is impossible that the US has been unaware of this center as a torture and death camp since 2011. In fact, the US government is consistently, if not constantly, made aware by satellite imaging of any new construction or activity occurring in and around Saydnaya.

## PART I: IRREGULAR WARFARE

### Out of the Blue: Wargames and Wars

The Arab Spring of 2011 was irregular warfare orchestrated by the US against Arab societies. In this section on wargaming, the reader will observe that the US military has been training for two decades in irregular warfare. The significance of discussing military wargaming is to show in three points that:

1) Tech companies and protesters did not act alone but alongside the Pentagon and the rest of the US intel-security state which is regularly conducting irregular warfare as official policy;

2) Wargaming is a misnomer - wargames are in fact practice for definite future military involvement or may act as cover for simultaneous real military action, and;
3) Wargames/continuous simulated warfare act as continuous real irregular warfare.

I am suggesting here in the section Out of the Blue: Wargames and Wars that many of those in the US policymaking and wargaming industries, especially those that have a hand in both, are disruptive actors employing irregular warfare with the willingness to recreate catastrophic events in the US as they have done abroad under the guise of wargaming.

**Unusual Games**

This section depicts the *cruel and unusual* side of wargaming. It describes the military deceptions of irregular warfare training which are used to train the intel-security state to act as enemy combatants. The role of news media in wargaming is discussed, as well as the public effect of wargame conduction and how it historically has created actual states of war. I show how the wargaming community deliberately mobilizes technology and people in information warfare operations disguised as wargames which are used to start wars, stage coups, and achieve other policy objectives. In a tactical assessment, the section details US military wargame preparations for domestic warfare, and compares the 2019 pandemic response to the US-led urban operations in Mosul in 2016.

**Horseshoes and Hand Grenades**

Real world events are exact recreations of wargames scenarioed years earlier in war colleges, think tanks, and intelligence reports. This section details an extensive comparative list of recent examples.

**Mind The Gap**

During wargame or disaster exercises, the simultaneous advent of an attack based on the precise scenario rehearsed points directly to persons aware of the scenario's plot as the perpetrators of the attack. As most attacks that attract media and political response are large attacks which required elaborate preparation beginning weeks or years earlier, the persons plotting the attack must be previously informed of the scripted exercise and wish to use the exercise as a smokescreen. Alternatively, it is possible authorities rehearsing the exercise became aware of a real-world plot, provided a smokescreen for the attack in the form of a simultaneous exercise and permitted the attack to occur. This is done to elicit a political reaction and therefore constitutes terrorism. The simultaneous conduction of exercises mimicking the precise attacks that occurred during the July 7, 2005 London Underground bombings and the September 11, 2001 hijackings are addressed in this section.

**'A Live Exercise'**

Secretary of State Mike Pompeo has stated of the COVID-19 pandemic that "We're in a live exercise", meaning disaster scenario or wargame exercise. The COVID-19 pandemic is approached in this section as intentional nuclear-biological-chemical (NBC) warfare that was wargamed. The premise of this approach is a 2008 National Intelligence Council's *Global Trends 2025* policy scenario. The NIC scenario predicted the failure to create a vaccine against a pandemic disease in which "tens to hundreds of millions of Americans within the US Homeland would become ill and deaths would mount into the tens of millions. Outside the US, critical infrastructure degradation and economic loss on a global scale would result as approximately a third of the worldwide population became ill and hundreds of millions died…".

### Lessons Learned

When the negative results of wargames recreated are in the real world, they are portrayed conciliatorily to the public as unprecipitated events which can still provide "lessons learned". The specific rhetoric "lessons learned" is indicative of a deliberate process used in intel-security industry to create trillion-dollar research and development funding opportunities out of disasters planned and executed by the same industry.

### Past is Prologue

The failure of wargaming to be applied as a preventative strategic-tactical measure against devastating developments deprives the practice of credibility. This extends to fields of research and development. Instances are discussed in which analysts accurately predict the past (termed "hypothetical past" in analysis reports), revealing a process in which foreknowledge of damaging events may be admitted *post facto* for profit. In short, this process allows analysts to recycle wargame plots as analysis.

## The Spectacular Security State

This section discusses the role of spectacle, media, and fiction in the intel-security state. I divide these into uses of media spectacle and speculative fiction.

This section focuses heavily on the misappropriation of surveillance technology as a tool for media production. This includes the *spectacularization* of real-world events under surveillance for the purpose of creating policy change, along the lines of the CNN effect. It also includes the *fictionalization* of real-world events under surveillance for the purpose of deception operations and financial exploitation, in which real surveillance operations are portrayed as entertainment media. Policy change, deception operations, and financial exploitation encourage the extension of unnecessary and transgressive surveillance.

### 'Total' Speculative Fiction

This subsection traces the origins of implausible, exaggerated speculative fiction used in defense planning to the precept of *total war* - both creativity and total war being concepts of modern warfare laid out by Clausewitz. In the modern US defense industries, the concepts have been combined to create the phenomenon in war planning I term *total speculative fiction*. Total speculative fiction is fictionalized defense scenario-making which grows increasingly violent and nondependent on reality, promoted by the expectation of total war.

### 4th Branch, 4th Group

Although not wargame scenarios proper, media spectacle constitutes a lesser discussed genre of fictionalized policymaking which employs mass communication and the dramatic arts, likened to the Armed Forces speculative fiction. Intelligence and military sectors identified with psychological/propaganda operations are identified as creators and enactors of media which propel policy and war.

### The Great Game

The Great Game is readily understood as the long series of political and military espionage, wars, coups, colonizations, assassinations, and policy deceptions which took place between world powers, including mercantilist companies, in the Near East during the 19th and 20th centuries. In this approach, wargames are part of an antiquated form of policy endeavor, especially obvious when taking place in the Near East. The

National Intelligence Council writes in 2008 that "in the case of Central Asia, where large deposits of energy resources [are, it will] increase the potential for a repeat of the 19th century's 'Great Game'."

## Monopoly on Violence, Monopoly on Infringement

The perceived inability of 'them to govern themselves' is a trademark of imperial thought discussed in post-colonial studies. In this section I point out that this perceived lack of legitimacy is the foundation for the US or other hegemons to authorize ('legitimize') violence in other nations.

Those with the state monopoly on violence are the same who hold what I call the monopoly on infringement. In this essay, as in Weber's *Politics as a Vocation*, the phrase refers to the right to infringe on the State's monopoly on violence. I use monopoly on infringement to also refer to infringement in the judicial sense of 'non-violent breach, encroachment or transgression'. The blurred line between the monopoly on violence and monopoly to infringe in the Information Age and in irregular warfare conduction is explored in this section.

The ability to alter and control perception is part of what I call here a 'monopoly on infringement'. Perception of an inability to self-govern is the legitimization for transnational use of force. The actual imposition of violence reinforces the perceived lack of legitimacy. Likewise, the ability to impose violence forces a perception of legitimacy.

### Monopoly on Infringement

Monopoly on infringement practicably refers to permission given by the State to non-governmental actors to commit non-violent crimes with full knowledge that the infringement may lead to violence. Infringements take the form of bulk data mining, surveillance, cyber-trespassing, cyber-theft, invasion of privacy, disregard of sovereignty, identity theft, assuming another's identity, slander and libel, copyright infringement, falsification of information, withholding of national security information, intentional security breaches, and other infringements regularly practiced and sanctioned by the State in the Information Age which can lead to violence.

### The VNN Effect

The VNN effect is the use of wargames and scenario-based media to set policy agendas, impede opposing agendas, and push decision-makers into action. 'VNN' is taken from the name of the mock news channel used in disaster scenario trainings by FEMA. While the CNN effect is understood to be the use of authentic news stories to alter policy agenda and action, by terming this phenomenon *the VNN effect*, I trace the media used under CNN effect conditions to their wargame/scenario origins. The media used in the VNN effect are based on speculative fiction created by policy and military industries, unlike media used to create the CNN effect, which are understood to be true but promoted for political purposes. Like the CNN effect, the VNN effect is used to propel nations into war.

In The VNN Effect, it is further shown that media are regularly used, without the informed consent of the public, as *the Public Space* for the manipulative wargaming of real-life situations and crises. That is, what is alleged to be comprehensive coverage of current events, or mere fictional entertainment, is actually used as the Public Space (a wargame term), "a central place to display and update information relevant to the game." Through fictionalized news media, the public is non-consensually involved as participants in wargame scenarios almost constantly which they experience as real-life.

### Cyber Realism

Within the paradigm of cyber realism, the exercise of monopoly on infringement to exercise violence must refer to the State that is actually in control of the three elements of Clausewitz's triad of war: operational instruments, popular passions, and policy. If it is shown that there is significant ability or disability for a state or person to control either instruments, public opinion, or policy, then that fact must be taken into account to determine actual monopoly-holder status.

An unfortunate starting point of this book has been the need to argue that the Arab Spring was decidedly damaging to the Arab countries involved, and the democratic reforms – if they really ever were attempted - were abject failures followed by unimaginable human tragedy. Because the real-life consequences can be so compelling, politicking our understanding of cyber operations is argued against under cyber realism.

## The Satellite Empire

In the context of cyber politics, cyberspace and cyber arms - alternatively called nuclear defense technology architecture and the global telecommunications grid - constitute the periphery of the US empire. Current events and cybertechnology are analyzed in this section to substantiate the sovereignty of an extant (and literal) 'Satellite Empire'.

### The Balance of Terror

Changes in the nuclear détente of geopolitical order, the 'delicate balance of terror', owed to cyberarms race practices and capabilities which have gone ignored for decades have possibly invalidated strategic concepts of deterrence, proliferation, and disarmament. Realities may have even nullified the very concept of *strategic* nuclear weapons. The geopolitical implications of the exploitation of these ambiguities and the increased exercise of that weapons system is presented as a major geopolitical threat.

### The Hacker's Arsenal

The lesser-known capabilities of cyberarms, the risks inherent in these weapons systems, and so-called man-in-the-middle problems (malicious authorized and unauthorized uses) of cyberwarfare systems are covered in this section.

### Radio-logical Warfare

Each and every technological weapon has a double life, so to speak, between weapons program briefs and psychological strategy boards. The purpose of delineating this section from the previous section The Hacker's Arsenal, which focused on the technical capabilities of cyberwarfare, is to highlight the Janus-faced nature of weapons systems. Rarely are technological weapons discussed in one venue as both weapons of physical destruction and societal destruction.

### The Capital of the Secret

Secrecy, corruption, inertia and 'active denial' policies meant to anonymize cyberarms/surveillance operations are analyzed as having led to the nullification of the US and foreign governments' legitimacies. The natural solution to the existence of an essential but unincorporated warfaring 'satellite empire' to a centralized empire is twofold. First, low-level accountability and individual case resolution according to existing legal judgements would be necessary. Second, at the national level the centralized government would need to make necessary reforms to bureaucratize and administrate the 'satellite empire' - crossing the Augustan threshold by integrating the expanding periphery into the bureaucracy functions of the center. This has failed to occur on either level. Because of this, individual injustices

continue to prevail, and the government's center ensures delegitimization and risks collapse. Rather, the course taken has been to increasingly monetize secrecy and surveillance.

### "The Bomb and the GNP"

This section argues that post-WWII international sovereignties and global economies are dictated by US national security interests. This section provides historical context to technology industries' conduct in the following sections Social Engineering and Proxy Wars and 'Going Native'. It provides historical backdrop for the more analytic section Recent Developments and Research and Development.

## PART II: THE ARAB SPRING

### Social Engineering

Hacking is predominantly social engineering - which is why the almost ironic impression others have of hacking culture is so important to foster, despite the obvious lame reality. Point-and-click level computer misusage does not garner reputation for excitement without serious propaganda efforts.

To describe the role of social engineering, RAND Corp. analyst Waltzman writes that "conscious and intelligent manipulation of the organized habits and opinions of the masses is an important element in democratic society. Those who manipulate this unseen mechanism of society constitute an invisible government which is the true ruling power of our country."

Media action often preempts military action by the US. As put forth in *The CNN Effect in Action*, media is used by policy planning staff to manipulate public opinion in order to achieve policy objectives. In this section, I focus on social media and broadcast media as harbinger of war.

#### Content and Platform Providers

In this section I show examples in which the full spectrum of the US telecom industry had to be aware and highly involved in the activities that led to the Arab Spring. Bahador, author of *The CNN Effect in Action* writes, "Such a connection is critical for the CNN effect, because it is important not only to demonstrate that the policy changed after such events, but to also link the policy change to the media images and framing of the events."

#### End Users

With a black suited faceless figure in front of a laurel-crowned globe, its logo looks like that of an off-brand intelligence contractor. Its Wikipedia history page reads like an index of CIA coups and military operations: Operation Payback, Operation Oklahoma, Operation Cartel, Operation Tunisia, OpSaudi, OpISIS. To much expressed internal dismay, the group admits the FBI instigated and coordinate the Occupy Wall Street movement in 2011 through it, resulting in the arrests of many of its protesters. And, in the same year, the group was at the center of a geopolitical watershed of revolutions and coups across the Middle East and beyond.

The trail of crumbs from the mostly failed Arab Spring movement and its results that lead directly to the cyber-social activities for which Anonymous took responsibility have found the media and academia nose-blind. Or, I will argue that Anonymous' broad proclamation "they are us, and we are them" is correct. This section identifies US federal agents, members of the media, academics and technologists as the creators of the Arab Spring movement of 2011.

## Proxy Wars and 'Going Native'

Technical proxy hacking is integral to social engineering and altering perceptions of political realities. This section describes how the coups and wars of the Arab Spring were incited/accomplished by manipulating Internet proxies, and therefore demographics of revolutionary politics, by presenting Western online protestors and agents as citizens of those Arab states in revolt. More precisely stated to facts presented in this section, the Internet-based opposition originally came *only* from outside the MENA region. The unusually high level of participation displayed by Westerners in the Arab Spring who otherwise do not concern themselves with events in the Middle East demands explanation.

### Internet Service Providers

Anonymous proclaimed in 2000 that "We are your SPs [Service Providers]." Even the coder who believes himself to be the most clever hacker is using a corporate Internet service provider like AT&T and Google to access the Internet, which in turn is organized under the authority of the US government's DNS. Today, domain and IP distribution and regulation online is under the control of ICANN, an American NGO under contract and supervision by the US Department of Commerce.

Many major content and platform providers have become Internet service providers as well, removing another important layer of competition that should serve as a buffer for user privacy. Despite sincere attempts at maintaining privacy through anti-malware software and even through private hardware, an end user or content provider must still go through an Internet service provider.

### Internet Backbone Providers

In *The CNN Effect in Action,* Babak Bahador writes that "Such models, like realism, assume unitary governmental decision-making with a high degree of control over implementation and access to near-perfect information," characterized by control of and information to the three domains necessary to war: "popular passions, operational instruments, and political objectives". Economist and former Director of Internet Policy Analysis of the FCC Michael Kende describes the physical reality of the Internet in the following passage:

"ISPs are generally connected to other ISPs through Internet backbone providers such as UUNET and PSINet. Backbones own or lease national or international high-speed fiber optic networks that are connected by routers, which the backbones use to deliver traffic to and from their customers. Many backbones also are vertically integrated, functioning as ISPs by selling Internet access directly to end users, as well as having ISPs as customers. Each backbone provider essentially forms its own network that enables all connected end users and content providers to communicate with one another. End users, however, are generally not interested in communicating just with end users and content providers connected to the same backbone provider; rather, they want to be able to communicate with a wide variety of end users and content providers, regardless of backbone provider. In order to provide end users with such universal connectivity, backbones must interconnect with one another to exchange traffic destined for each other's end users. It is this interconnection that makes the Internet the 'network of networks' that it is today." In *The Politics and Technology of Cyberspace*, lecturer of strategy and defense Daniel Steed writes, "whoever can master, control, and exploit the submarine cables to best effect will develop a very valuable geopolitical advantage."

## Recent Developments and Research and Development

The funding cycle of violence, shocking developments publicized will result in more demand for research and development, part of the cyclical mechanism described in this section. Mutual perpetuation of R&D and 'bad policy' is self-evident in modelism and the state of arrested political and scientific development.

### The Bosnia Model, The Rumsfeld Model

In academic discourse models are used to detail an instance of methodology or best practices for the purpose of instructing others how to recreate a successful experiment or policy. I will show here that the Yugoslav War (1991-1995) and genocide in Bosnia has become a model used by US politicians and foreign policy advisors for more recent wars involving the US and NATO. I point out the Bosnia model in order to show that its recreation, with all the devastating consequences throughout various regions of the world, is deliberate policy failure.

In *Succession Management for Senior Military Positions The Rumsfeld Model for Secretary of Defense Involvement* (2011), RAND Corporation analysts describe what they term 'the Rumsfeld Model': "When, for development purposes, an individual is deliberately placed in a position for which there were better-qualified candidates, the placement will best benefit the organization if it is part of a carefully considered career path."

Awareness of the deliberate misuse of modeling can prevent the continued recreation of devastating and insidious policy if informed action is taken to prevent the policy from being enacted.

### Research and Arrested Development

Mutual perpetuation of R&D and 'bad policy' is self-evident in the state of arrested political and scientific development.

While the news media is what has been discussed as the prime medium for propelling wartime philosophies, Jean Baudrillard wrote in 1993 in *No Pity for Sarajevo* on the spectacularization of human suffering for legitimating intellectual-political action (i.e. research and development) - "the one serving up its corruption and scandals, the other its artificial convulsions and inertia… offerings in a televisual holocaust":

> "Everywhere we look distress, misery, and suffering have become the raw goods… Those who do not directly exploit it do so by proxy, and there is no dearth of middlemen skimming a financial or symbolic profit along the way. As with global debt, deficits and suffering are negotiable and have resale value on the futures markets - here, the intellectual-political markets - which are the present-day equivalents of the military-industrial complex of the sinister old days. The logic of suffering governs all commiseration. Even if we mean to confront suffering, our very reference to it gives suffering an indefinite base of objective reproduction. Clearly, to combat anything, one's starting point must be the evil underlying suffering."

The evil Baudrillard addresses here is the commodification of suffering. In an example of what could be studied as late-stage capitalist vertical integration, he accuses intellectuals, politicians and media of "serving up corruption and scandals" as well as being the same who cause global civil unrest and violence through "its artificial convulsions and inertia." This is a philosophical underpinning of the argument made by Babak Bahador in *The CNN Effect in Action*.

MAXAR Satellite Technology VP of Communications Nancy Coleman has stated, "The visual context that we provide puts a compelling spotlight on injustice and human suffering allowing decisions to be made with

confidence and is an extension of Maxar's purpose." Coleman's statement clearly outlines MAXAR's production line, from injustice and human suffering to satellite imaging, to news media, to policy decision-making. She clarifies that injustice and human *suffering is the product* sold by satellite imaging companies like MAXAR. This is the socio-political system which I am calling for cyber realism to be applied to.

In example, the 2020 House Foreign Affairs Committee on Afghanistan Reconstruction Special IG John Sopko concluded testimony with a call for US support to be given to the Taliban rather than the Afghan national government. Within his statement is a call for more funding for research and development to correct the incorrect government research based on "fudged statistics" which already cost the US $133 billion dollars. Despite his saying that the source of bad statistics and decisionmaking is due to the fact that "first they classified the data, then they stopped reporting it. You as members of Congress have no public metrics to rate the billions of dollars we are spending in Afghanistan," the special IG calls for more funding for classified research and development to support a policy shift that would return US policy to a Cold War position supporting armed mujahidin fighters.

Inevitably, at the media level this recent 'embarrassing' development before the House and public will result in increased public demand for responses and solutions, i.e. research and development, with a retroactive policy course already waiting in the wings. This exemplifies the entropic mechanism at work detailed in the final section Research and Arrested Development.

**Conclusions**

If global connectedness is any indicator, the scourge of telecommunication shadow governments rivals early modern colonialism in scale and could forewarn of global power shifts. These global power shifts may expand surveillance-colonial governance models, or, power shifts via hackers' wars may forewarn of the collapse of the US 'satellite empire' and surveillance States.

**The Greater Middle East Plan**

In a separate research paper still in the planning phase tentatively titled "The Historicism of the Greater Middle East Plan", I suggest that the political philosophy driving the scripted, total, quick-paced destabilization and destruction of the Middle East arises from a school of political thought known as political messianism, or millenarianism, - a secular political philosophy highly informed by religious eschatology and the compulsion to bring about the Armageddon by fulfilling apocalyptic prophesies in the real world.